

STATEWIDE INFORMATION SYSTEMS POLICY

Statewide Policy: Disposal of Computers

Product ID: ENT-SEC-141

Effective Date: August 3, 2005

Approved: Janet R. Kelly, Director, Department of Administration

Replaces & Supersedes: This policy supercedes any prior enterprise policies for establishing and implementing information technology (IT) policies and standards.

I. Authorizations, Roles, & Responsibilities

Pursuant to the Montana Information Technology Act ("MITA") (Title 2, Chapter 17, Part 5 of the Montana Code Annotated ("MCA"), it is the policy of the state that information technology be used to improve the quality of life of Montana citizens, and that such improvement is to be realized by protecting individual privacy and the privacy of the information contained within the state's information technology systems. [§2-17-505\(1\), MCA](#). It is also the policy of the state that the development of information technology resources be conducted in an organized, deliberative, and cost-effective manner, which necessitates the development of statewide information technology policies, standards, procedures, and guidelines applicable to all state agencies and others using the state network. It is also anticipated that State information technology systems will be developed in cooperation with the federal government and local governments with the objective of providing seamless access to information and services to the greatest degree possible. [§2-17-505\(2\), MCA](#).

Department of Administration: Under MITA, the Department of Administration ("DOA") is responsible for carrying out the planning and program responsibilities for information technology for state government (except the national guard), including for establishing and enforcing a state strategic information technology plan and establishing and enforcing statewide information technology policies and standards. DOA is responsible for implementing MITA and all other laws for the use of information technology in state government. The director of DOA has appointed the chief information officer to assist in carrying out the department's information technology duties. [§2-17-512, MCA](#).

Department Heads: Each department head is responsible for ensuring an adequate level of security for all data within their department. [§2-15-114, MCA](#).

II. Policy - Requirements

A. Scope

This policy applies to all state agencies of the Executive branch; and, by adoption, the Judicial and Legislative branches. This policy does not apply to the Montana University System or the Office of the Commissioner of Higher Education.

This policy applies to personal computers, other computing devices, and accessory equipment that store electronic data, information, and software programs.

B. Purpose

When disposing of information technology (IT) equipment, agency directors have a responsibility to assure that sensitive information is protected. Additionally, licensed proprietary software must be protected against unauthorized distribution. Sensitive information includes data required by law to be protected from disclosure to individuals and entities both inside and outside of state government. This policy outlines disposal requirements for protecting these IT assets by either of two methods: (1) destruction of the IT device; or, (2) complete removal of all electronic data from the computer storage device. The state agency must perform at least one of these actions before disposing of the device.

C. Definitions

Disposal - The authorized removal of an IT storage device from an agency's control or possession, regardless of the means by which this is accomplished.

Computer Storage Device – Includes, but is not limited to: personal computers with hard drives, servers with hard drives, other assets with hard drives or loose/unattached hard drives.

Sanitize - A process used to assure that data is destroyed or removed from an IT storage device. This may be achieved by physical destruction of the device or by the proper use of specialized software utility programs that overwrite the data so that it is unrecoverable. Note: This sanitizing process is also known as a "cleaning" process.

Removable storage Media – Includes, but is not limited to: floppy diskettes, compact disks (CD's), magnetic tapes, digital video devices (DVD's), Zip media, and Flash media.

Physical Destruction – To incinerate, pulverize, shred, or melt the computer storage device or component that is capable of storing electronic data or software programs.

D. Disposal Requirements

All computer storage devices must be sanitized prior to disposal, regardless of where the agency chooses to dispose of them. State agencies and their employees shall follow these requirements when disposing of a computer storage device or removable storage media.

All agency data and software programs must be removed from the hard drive prior to its disposal; or, alternatively, the hard drive must be destroyed. To remove data and software, agency IT personnel should use a Department of Defense (DoD) 5220.22-compliant sanitation program that will effectively sanitize the hard drive. The program uses the DoD “three-pass” process to: (1) overwrite all electronically addressable locations on the device with a character; (2) overwrite it again with the same character’s complement bit configuration; and then (3) overwrite it again with a random character. Finally, the program will perform a verification process to assure that the sanitizing has been accomplished.

If the data storage device cannot be put through this process because it is not functional, the device must be physically destroyed. Software products are available, both freeware and purchased, that comply with DoD requirements for storage sanitation. [Click here](#) for a list of acceptable products.

All removable storage media must be physically destroyed.

Agency directors are responsible for maintaining documentation on all electronic data storage devices (e.g., PCs, laptops, servers, PDAs) that have been either destroyed or sanitized. These records must be retained by the agency for two years.

The disposal records shall contain the following information:

- Device identification (vendor serial number or Dell service tag number)
- Date of cleaning
- Employee name performing cleaning
- Method of cleaning
- Destination of device (surplus, landfill, etc)
- Disposing Agency

All computer storage devices must be sanitized prior to disposal, regardless of where the agency chooses to dispose of them. Agencies disposing of equipment through the Property and Supply Bureau’s Surplus Equipment program or by donating their surplus functional equipment to the Office of Public Instruction (OPI) should contact these entities for a copy of their additional requirements.

E. Background - History On The Creation Of Or Changes To This Policy

The Information Technology Security Office of the Information Technology Services Division created this policy. Information contained in this policy originated from the Section 1-0250.00, MOM.

This policy was revised in June of 2005 to adopt the Department of Defense three-pass disk sanitation process and requires agency record-keeping of computer disposals. Additionally, the scope of the policy was expanded to include all IT Data Storage Devices.

F. Change Control and Exceptions

Policy changes or exceptions are governed by the Procedure for Establishing and Implementing Statewide Information Technology Policies and Standards. Requests for a review or change to this policy are made by submitting an [Action Request](#) form. Requests for exceptions are made by submitting an [Exception Request](#) form. Changes to policies and standards will be prioritized and acted upon based on impact and need.

III. Close

For questions or comments about this instrument, contact the Information Technology Services Division at [ITSD Service Desk](#), or:

Chief Information Officer
PO Box 200113
Helena, MT 59620-0113
(406) 444-2700
FAX: (406) 444-2701

IV. Cross-Reference Guide

A. State/Federal Laws

- [2-17-505\(1\)](#) – Policy
- [2-17-514\(1\)](#) – Enforcement
- [§2-17-505\(2\), MCA](#)
- [§2-17-512, MCA](#)
- [§2-15-114, MCA](#)
- MCA 2-17-532-534
- MCA 2-15-114

B. State Policies (IT Policies, MOM Policies, ARM Policies)

- [2-15-112, MCA](#)
- [ARM 2.13.101 - 2.13.107](#) - Regulation of Communication Facilities
- This policy (ENT-SEC-141) replaces policy ENT-SEC-140 effective August 2, 2005.
- [MOM 3-0130 Discipline](#)
- [ARM 2.12.206](#) Establishing Policies, Standards, Procedures and Guidelines.

C. IT Procedures or Guidelines Supporting this Policy

- [Policy: Establishing and Implementing Statewide Information Technology Policies and Standards](#)
- [Procedure: Establishing and Implementing Statewide Information Technology Policies and Standards](#)
- “Recommendations for Disposal of Computers” created by the Information Security Committee.
- Surplus Property guidelines

V. Administrative Use

Product ID:	ENT-SEC-141
Proponent:	Janet R. Kelly, Director, Department of Administration
Version:	1.1
Approved Date:	July 15, 2008
Effective Date:	August 3, 2005
Change & Review Contact:	ITSD Service Desk
Review Criteria:	Event Review: Any event affecting this policy may initiate a review. Such events may include a change in statute, key staff changes or a request for review or change.
Scheduled Review Date:	July 1, 2013
Last Review/Revision:	Reviewed July 11, 2008. Non-material changes are necessary.
Change Record:	July 11, 2008 – Non-material changes made: <ul style="list-style-type: none">- Standardize instrument format and common components.- Changed to reflect next review date.